SOPHOS
Security made simple.

Solution Brief: Next-Generation Endpoint Security

Für Next-Generation Endpoint Security gibt es viele verschiedene Definitionen. Manche Anbieter setzen auf Insellösungen, die jeweils nur eine ganz bestimmte Aufgabe übernehmen, z. B. Exploit Prevention oder Bedrohungserkennung, während andere Next-Generation Endpoint Security ganzheitlich angehen. In diesem Solution Brief erklären wir, welche Verfahren Sophos in den drei Hauptbereichen einer Next-Generation Endpoint Security – Abwehr, Erkennung und Reaktion – anwendet.

Abwehr: Das Kernziel von Abwehrmaßnahmen besteht darin, zu verhindern, dass Unbefugte mit unlauteren Absichten Zugang erhalten oder Software auf einem geschützten Gerät ausführen können. Es geht darum, geeignete Barrieren zu implementieren, die Angreifer daran hindern, ihre böswilligen Absichten in die Tat umzusetzen – sei es Datendiebstahl oder eine Betriebsstörung.

Next-Generation-Endpoint-Security-Produkte, die nicht gleich zu Beginn den Zugang zum Gerät unterbinden, verpassen damit bereits eine wertvolle Gelegenheit, wichtige Ressourcen zu schützen.

Erkennung: Angreifer nutzen oft Schwachstellen in autorisierten Anwendungen, und Benutzer können versehentlich oder vorsätzlich Schadsoftware installieren. Deshalb muss der Endpoint erkennen, wenn die Abwehr versagt hat. Eine bloße Erkennung der Bedrohung ohne eine darauf folgende Reaktion ist jedoch nur von forensischem Wert und wird unseren Anforderungen an ein Next-Generation-Security-Produkt nicht gerecht. Schädliche Aktivitäten müssen gleich nach ihrer Erkennung gestoppt werden.

Reaktion: Wurden schädliche Aktivitäten erkannt, muss der Endpoint in der Lage sein, Maßnahmen zu ergreifen: nicht nur, um den Angriff zu stoppen, sondern auch, um jegliche bereits vorhandene Malware zu entfernen und den Administrator über die Einzelheiten des Ereignisses zu informieren. Administratoren müssen schnell verstehen können, was gerade erkannt wurde, welche Ursache das betreffende Ereignis hat, welche Daten gefährdet wurden, welche Komponenten des Systems betroffen waren, was sie tun können, um einen Angriff in Zukunft zu verhindern und ob die Komponenten der schädlichen Aktivitäten auch auf anderen Geräten Fuß fassen konnten. Nur so ist eine effektive Reaktion auf Vorfälle gewährleistet.

Abwehr

Für eine erfolgreiche Abwehr ist es entscheidend, dass die Malware daran gehindert wird, auf dem Gerät Fuß zu fassen. Wenn die Abwehr funktioniert, können Administratoren darauf vertrauen, dass keine weiteren Maßnahmen erforderlich sind. Der Angreifer konnte nicht bis zum Gerät vordringen und Daten wurden nicht gefährdet.

Es gibt zwei grundlegende Verfahren, die angewendet werden können, um zu verhindern, dass Malware auf einem Endpoint Fuß fassen kann: Exposure Prevention und Execution Prevention. Beide Verfahren stützen sich auf eine Vielzahl von Technologien.

Exposure Prevention

Exposure Prevention verhindert proaktiv, dass Benutzergeräte mit Malware oder sonstigen schädlichen Aktivitäten in Berührung kommen. Bei Sophos bieten wir drei Kerntechnologien zur Exposure Prevention an: Web Protection, Device Control und Patch-Analyse.

Web Protection: Die Sophos Endpoint Protection Agents nutzen SophosLabs-Daten über bekannte Malware-, „Command and Control"- und Exploit-Websites, um eine Navigation zu diesen Bedrohungsherden zu unterbinden. Zusätzlich zu Bedrohungsdaten auf dem Gerät selbst kann der Endpoint mittels Sophos Live Protection Echtzeit-Informationen über Schad-URLs abrufen. Die Liste der Schad-Websites wird ständig aktualisiert und die SophosLabs nutzen zur Pflege ihrer Datenbank bekannter schädlicher Adressen sowohl selbst entwickelte Verfahren als auch Branchenfeeds. Sophos verhindert nicht nur, dass der Browser zu einer verdächtigen Website navigiert, sondern scannt den Inhalt der Seite auch auf schädlichen Umleitungscode und kompromittierte Elemente (z. B. schädliche Flash-Objekte und Javascripts).

Device Control: Eine weiteres Exposure-Prevention-Verfahren für Endpoints ist die Verwaltung und Kontrolle angeschlossener Medien wie USB-Sticks. Die Sophos Endpoint Protection Agents ermöglichen Administratoren, Richtlinienkontrollen zu erstellen und zu pflegen, mit denen einzelne Geräte explizit erlaubt und anpassbare Regeln angewendet werden können, sobald ein Gerät erkannt wird.

Patching: Eine der besten Methoden zum Schutz eines Endpoints vor Angriffen besteht darin, sicherzustellen, dass alle Sicherheitspatches sowohl für das Betriebssystem als auch für sämtliche auf dem Gerät installierten Anwendungen angewendet wurden. Dies ist ein wichtiger erster Schritt, der dafür sorgt, dass die einem Angreifer zur Verfügung stehende Angriffsfläche insgesamt verkleinert wird. Bei vielen Angriffen werden Schwachstellen in seriösen Geschäftsanwendungen ausgenutzt, und die meisten Angreifer sind in der Lage, in kürzester Zeit Exploit-Software zur Ausnutzung bekannter Schwachstellen zu entwickeln. Deshalb müssen IT-Sicherheitsteams unbedingt dafür sorgen, dass Software-Updates immer zeitnah eingespielt werden. Den Patch-Status stets auf dem aktuellen Stand zu halten, fällt größtenteils in den Aufgabenbereich „allgemeine Geräteverwaltung“ und darf darin nicht aus dem Blickfeld verschwinden. Um Kunden diese wichtige Aufgabe zu erleichtern, bietet Sophos eine Extra-Funktion zur Analyse des Patch-Status.

Neben Exposure-Prevention-Verfahren, die auf dem Endpoint ausgeführt werden können, gibt es weitere Abwehrmethoden, z. B. sichere Benutzerauthentifizierung, E-Mail-Filterung sowie Einsatz von Firewalls und UTM-Appliances. Sicherheitsteams können verschiedenste Schutzmaßnahmen ergreifen: Erkennung und Abwehr von Phishing-Angriffen, die dem Einschleusen von Malware dienen, Blockierung des Zugriffs auf Blacklist-URLs und weitere Methoden bis hin zur physischen Isolation des Geräts vom Internetzugang und dem Verkleben des USB-Anschlusses mit Sekundenkleber.

Beim Vergleich unterschiedlicher Next-Generation-Endpoint-Security-Produkte sollten Sie unbedingt darauf achten, welche Funktionen zur Exposure Prevention geboten werden. Viele Neueinsteiger am Markt ignorieren diesen Aspekt der Next-Generation Endpoint Security komplett. Einige vertreten die Ansicht, dass Sie Ihre Benutzer ohne Bedenken auf alles klicken lassen können. Andere verlassen sich beim Schutz auf eine Firewall, was jedoch nur funktioniert, wenn das Gerät sich im geschützten Netzwerk befindet.

Execution Prevention

Dass ein Endpoint früher oder später mit Malware konfrontiert wird, ist unausweichlich. Welche Technologien können in einer solchen Situation die Malware identifizieren und blockieren, bevor sie ausgeführt werden kann?

Execution Prevention umfasst eine Reihe interessanter Technologien und beinhaltet herkömmliche Abgleiche mit Signaturen bekannter Malware, heuristische Auswertung, Emulation, Sandboxing, Dateireputation-Scoring, Anwendungs-Whitelisting und eine Vielzahl von Machine-Learning-Algorithmen, die anhand statistischer Mathematik ermitteln, ob eine Datei unbedenklich oder schädlich ist.

Heuristische Auswertung: Eine heuristische Auswertung kann sowohl bekannte Malware als auch neue, noch unbekannte Malware abfangen. Da heuristische Modelle in der Lage sind, Zero-Day-Malware und unbekannte Malware-Varianten zu erkennen, müssen sie regelmäßig aktualisiert und angepasst werden, um False-Positive-Erkennungen zu vermeiden. Bei Sophos-Produkten muss der Administrator die Regeln und Erkennungsmodelle nicht selbst pflegen. Die sofort einsatzbereite heuristische Engine von Sophos ist bereits auf maximale Erkennungs- und minimale False-Positive-Raten optimiert und wird von den SophosLabs mit automatischen Modellanpassungen immer auf dem neuesten Stand gehalten.

Die heuristische Engine von Sophos prüft jede Sample-Datei auf Codeabschnitte, die darauf hindeuten, dass die Datei andere Dateien löschen, Registry-Änderungen vornehmen, andere Dateien installieren, verschlüsselten Ausführungscode nutzen und ähnliche Aktionen durchführen könnte. Heuristische Erkennungsverfahren sind Teil des Mechanismus, den Sophos zur Erkennung von Malware anwendet. Beim Anlegen von Algorithmen zur heuristischen Malware-Erkennung ist es entscheidend, die richtige Balance zu finden: Einerseits müssen schädliche Eigenschaften zuverlässig erkannt werden und andererseits darf unbedenkliche Software, die zufällig über ähnliche Eigenschaften wie Malware verfügt, nicht als schädlich eingestuft werden. Dieser Prozess der Algorithmus-Abstimmung ist der Punkt, an dem die Balance zwischen Erkennung und False Positives zum Tragen kommt. Wenn die Abstimmung der heuristischen Regeln zu streng ist, werden zu viele Elemente abgefangen (Malware und Nicht-Malware) und die Regeln verlieren ihre Fähigkeit, zukünftige Varianten zu erkennen. False Positives ist der Bereich, in dem viele der neueren Endpoint-Security-Produkte schlichtweg nicht an das Niveau etablierter Lösungen herankommen und häufig über Wochen eingerichtet und kontinuierlich von IT-Sicherheitsadministratoren angepasst werden müssen.

Emulation vor Ausführung: Der Sophos Endpoint Protection Agent verfügt über einen Geräteemulator, der ausführbare Dateien in einer kontrollierten Umgebung ausführt. Der Emulator dient vorrangig dazu, Malware zu identifizieren und verschlüsselte Ausführungskomponenten sichtbar zu machen sowie Kompromittierungsindikatoren (z. B. Registry-Änderungen und Zugriff auf andere Dateien/Anwendungen) zu sammeln. Nach Identifizierung der Malware kann der Sophos-Endpoint eine gründlichere heuristische Auswertung der nun sichtbaren Komponenten vornehmen.

Sandboxing: Die SophosLabs verfügen über ihre eigene Sandbox, in der Samples von Branchenfeeds, aus unserem eigenen Honeypot-Netzwerk und von Kunden-Endpoints ausgewertet werden. Die Ergebnisse aus der Sandbox dienen Datenwissenschaftlern und Bedrohungsanalysten als Orientierungsgrundlage bei der Erstellung von Regeln sowohl für Abwehrmodelle als auch für komplexere Modelle zur Verhaltenserkennung. Updates durchlaufen eine Testphase, um ihre Wirksamkeit, Effizienz und minimale False-Positive-Rate zu bestätigen, bevor sie automatisch auf allen Endpoints angewendet werden.

Download-Reputation: Durch die Reputationsprüfung bei Downloads hat die Sophos Endpoint Protection die Möglichkeit, mit dem Endbenutzer zu interagieren, wenn eine verdächtige ausführbare Datei auf das Gerät heruntergeladen wird. Sollten wir den Download einer hochverdächtigen Datei beobachten, die bislang weder als schädlich noch als unbedenklich klassifiziert wurde, können wir den Benutzer fragen, ob er den Download fortsetzen möchte oder nicht. Als wie verdächtig eine heruntergeladene ausführbare Datei eingestuft wird, hängt von einer Reihe von Faktoren ab, u. a. vom Ursprung der Datei, wie häufig die Datei bereits von unseren Systemen erfasst wurde, ob sie von einem renommierten Softwarehersteller stammt, von den Crowd-Sourcing-Ergebnissen darüber, wie andere Benutzer auf die Frage reagiert haben, ob sie den Download der Datei fortsetzen möchten, sowie von vielen weiteren Attributen. In den ersten drei Monaten nach Einführung der Reputationsprüfung bei Downloads wurden Risikobewertungen für über 70 Mio. ausführbare Dateien erstellt; die Liste wächst stetig weiter.

Anwendungs-Whitelisting: Die von Sophos bereitgestellte Technologie zum Anwendungs-Whitelisting heißt „Lockdown". Diese Technologie identifiziert die für einen Server zugelassenen Anwendungen, Dienste und Prozesse und verhindert, dass neue Elemente zur Whitelist hinzugefügt werden. Diese Technologie ist also eine wirksame Methode, um die Installation nicht autorisierter Anwendungen zu verhindern. Wie alle Technologien ist auch Whitelisting nicht DAS Allheilmittel, und Whitelisting auf Sophos-geschützten Endpoints ist daher nur ein Element innerhalb einer übergreifenden Next-Generation Endpoint Security.

Machine Learning: Bei diesem Verfahren werden bayessche Analysen, lineare Regression, Random Forests und weitere Algorithmen des maschinellen Lernens genutzt, um zu ermitteln, ob eine Datei aller Wahrscheinlichkeit nach schädlich ist oder nicht. Bei diesen Modellen muss der Algorithmus eine Übungsphase durchlaufen, in der er Hunderte bis Tausende erkannter Attribute als schädlich bekannter Dateien beobachtet. Anhand dieser Beobachtung ermittelt das Modell dann die Wahrscheinlichkeit, ob eines oder mehrere Attribute auf eine Schädlichkeit hindeuten. Sobald das Modell erstellt und die Gewichtung für jedes Erkennungsattribut festgelegt wurde, können Sie jede beliebige Datei zur Auswertung einreichen und der Algorithmus liefert Ihnen eine Entscheidung darüber, ob die Datei schädlich oder unbedenklich ist oder sich in einer Grauzone dazwischen befindet. Dieses Verfahren kam vor über einem Jahrzehnt erstmals flächendeckend in Anti-Spam-Lösungen zum Einsatz und hat seitdem seinen Weg in die allgemeinere Malware-Erkennung gefunden. Die SophosLabs nutzen eine Vielzahl von Machine-Learning-Algorithmen, um Schadsoftware zu erkennen und die Regeln und Modelle der im Agent enthaltenen Schutztechnologien anzupassen.

Signaturerkennung: Dass eine Signaturerkennung allein nicht mehr ausreicht, ist allgemein bekannt. Denn Signaturen sind darauf ausgelegt, ausschließlich bekannte Bedrohungen zu erkennen. Viele Infektionen sind inzwischen dateilos und nutzen Schwachstellen aus; andere nutzen polymorphe Malware, gegen die signaturbasierte Systeme praktisch machtlos sind. Als Einzeltechnologie ist eine Signaturerkennung daher keine effektive Lösung. Trotzdem hat die Signaturerkennung durchaus noch ihre Daseinsberechtigung. Denn Signatur-Technologie ist und bleibt eine kostengünstige und effektive Methode zum Schutz vor bereits bekannten Bedrohungen und bildet eine solide Sicherheitsgrundlage. In Kombination mit anderen in diesem Dokument beschriebenen Techniken ist Signatur-Technologie daher eine effektive und effiziente Endpoint-Schutz-Komponente.

Erkennung

Die Malware wurde entweder versehentlich oder vorsätzlich von einem Benutzer installiert. Ggf. hat sie eine Prozess-Schwachstelle ausgenutzt und die Kontrolle über einen legitimen Geschäfts- oder Betriebssystemprozess übernommen oder sie nutzt bestehende autorisierte Anwendungen direkt durch ein Skript, Social Engineering oder einen Fehler bzw. Vorsatz des Benutzers. Die Erkennung schädlicher Aktivitäten ist somit ein breites Feld und umfasst u. a. das Aufdecken von internen Bedrohungen, Identitätskompromittierungen und natürlich von Malware.

Bei der Erkennung von Malware muss beachtet werden, dass wir es unter Umständen nicht mit einer ausführbaren Malware-Datei zu tun haben, sondern mit einem Skript, das seriöse Software oder legitimen Code ausnutzt und durch einen Exploit direkt in einen laufenden Prozess eingeschleust wurde. Daher betrachten wir im Folgenden eine Reihe von Technologien, die zur Erkennung aktiver Schadsoftware eingesetzt werden, u. a. Monitoring des Netzwerkverhaltens, Monitoring des Anwendungs-/Prozessverhaltens, Datenschutz und Exploit-Erkennung.

Netzwerkverhalten: Monitoring des Netzwerksverhaltens wurde ursprünglich nur auf Firewalls oder mittels Aggregation von Netzwerkdaten in einem SIEM für Analyseprozesse angewendet. Durch Monitoring des Netzwerkverhaltens auf Endpoint-Ebene mittels Malicious Traffic Detection kann der Sophos-Endpoint die Kommunikationen mit externen Geräten auf Prozessebene beobachten und Kommunikationen zu verdächtigen „Command and Control"- bzw. anderen Malware-übertragenden Servern erkennen – sowohl, wenn der Endpoint sich im Unternehmenswerk befindet, als auch wenn das Gerät außerhalb des Netzwerks genutzt wird. Sophos nutzt Malicious Traffic Detection (Erkennung schädlichen Datenverkehrs), um zusätzliche Analysen des Prozesses auszulösen, der den Traffic generiert hat. Mit diesen Analysen kann Malware aufgedeckt werden, die andere Erkennungsverfahren überlistet hat.

Anwendungsverhalten: Zur Überwachung von Anwendungen auf schädliche Verhaltensweisen hat der Anbieter ein oder mehrere Bedrohungsmodelle mittels Machine Learning, heuristischen Experten-Regeln oder anderen Methoden entwickelt. Unabhängig von der zur Identifizierung bedrohlicher Verhaltensweisen angewandten Methode besteht das Kernziel darin, zu ermitteln, wann eine Anwendung eine als bedrohlich bekannte Aktion ausführt. Dies umfasst alles von der Interaktion zwischen Prozessen, der Registry und des Netzwerks bis hin zu spezifischen Methoden, die von einem Prozess für Verschlüsselung, Speicherzugriff, Puffer usw. genutzt werden.

Um bedrohliche Verhaltensweisen zu erkennen, muss ein Next-Generation-Endpoint-Security-Produkt zunächst sicherstellen, dass alle Laufzeit-Anwendungsaktivitäten erkannt und korreliert werden können. Die Beobachtung der Anwendungsaktivitäten kann mittels Kernel Hooking, Ereignisüberwachung, Process Injection oder anderen Methoden durchgeführt werden und muss unter Berücksichtigung der aktuellen Laufzeit und des Aktivitätsverlaufs der Anwendung erfolgen.

Angesichts der Tatsache, dass „bedrohliche" Verhaltensweisen von Anwendungen sich oft als legitime Aktionen von Geschäftsanwendungen herausstellen (z. B. sich mit dem Internet verbindende Word-Makros), muss der Anbieter nicht nur in der Lage sein, bedrohliche Verhaltensweisen zu erkennen, sondern auch verstehen können, ob die jeweilige Verhaltensweise oder Kombination von Verhaltensweisen ausreicht, um die Anwendung als schädlich einzustufen oder nicht. Wie ein Anbieter entscheidet, worüber Administratoren informiert werden und wann Software als schädlich eingestuft wird, kann bei der Verhaltensüberwachung zu großen Herausforderungen führen.

Im Gegensatz zu den vielen anderen Anbietern von Technologien zur Verhaltensüberwachung pflegen die SophosLabs die Modelle und Regeln, die für eine zuverlässige Erkennung von Malware notwendig sind. Unsere Kunden müssen demzufolge keine anspruchsvollen Trainingskurse absolvieren und keine komplizierten Konfigurations- und Außnahmeeinstellungen vornehmen, um das Produkt erfolgreich bereitzustellen.

Verschlüsselung: Mit dem Release von Sophos SafeGuard (SGN) 8.0 führen wir eine Datenverschlüsselungstechnologie ein, die nicht nur Festplatten und Dateien verschlüsselt, sondern auch die Vertrauenswürdigkeit einer Anwendung als Zugriffsvoraussetzung vorsieht. Das Produkt ermöglicht eine transparente Schlüsselverwaltung für vertrauenswürdige Anwendungen, sodass Benutzer verschlüsselte Dateien aufrufen und erstellen können, ohne ihr Verhalten ändern zu müssen. Der Administrator hat für SGN 8.0 eine Whitelist von Anwendungen konfiguriert, die auf verschlüsselte Materialien zugreifen dürfen. Wenn eine Anwendung nicht auf der Whitelist steht, bleiben die Daten verschlüsselt.

Zusätzlich zu Verschlüsselungsanforderungen auf Anwendungsebene sperrt SGN 8.0 bei einer Bereitstellung auf einem per Sophos Central verwalteten Endpoint Protection Agent wichtige Materialien, wenn der Endpoint oder die Sophos XG Firewall schädliche Aktivitäten erkennt. Eine dynamische Schlüsselsperrung auf Grundlage des geräteseitigen Sicherheitsstatus bietet nur Sophos an.

Exploit-Erkennung: Durch die Möglichkeit, Verhaltensweisen von Anwendungen zu überwachen, sind wir auch in der Lage, vertrauenswürdige Prozesse zu beobachten und zu erkennen, wenn diese von Malware missbraucht werden. Die Anzahl von Verfahren zur missbräuchlichen Nutzung eines Prozesses ist begrenzt und Malware nutzt größtenteils eines oder mehrere der folgenden Verfahren, um Exploit-Möglichkeiten auszuloten:

Exploit-Techniken

- Data Execution Prevention (DEP) – Verhindert, dass Exploit-Code vom Speicher ausgeführt wird
- Mandatory Address Space Layout Randomization (ASLR) – Erschwert das Vorhersagen von Codespeicherorten
- Null Page – Stoppt Exploits, die Sprungbefehle über die Zero-Page beinhalten
- Dynamic Heap Spray – Stoppt Angriffe, die verdächtige Sequenzen an verschiedene Stellen des Heaps schreiben
- Stack-basiertes Anti-ROP – Stoppt ROP(Return-oriented Programming)-Angriffe
- Hardware-gestützte Control-Flow Integrity (CFI) – Stoppt hochentwickelte ROP-Angriffe
- Import Address Table Filtering (IAF) – Stoppt Angriffe, die nach API-Adressen in der IAT suchen
- Stack Pivot – Stoppt missbräuchliche Nutzungen des Stack Pointers
- Stack Exec – Stoppt Code von Angreifern auf dem Stack
- Load Library – Blockiert Bibliotheken, die direkt aus dem Speicher oder von UNC-Pfaden geladen werden
- Shellcode – Stoppt Code-Ausführung in Gegenwart von Exploit-Shellcode
- Anwendungs-Lockdown – Stoppt Logic-Flaw-Angriffe, die Maßnahmen zur Risikominimierung umgehen
- Prozess-Schutz – Stoppt Angriffe, die Prozesse übernehmen oder ersetzen
- Man-in-the-Browser-Erkennung – Enttarnt Eindringlinge, die kritische Browser-Funktionen manipulieren

Weitere moderne Schutzverfahren

- Ransomware-Schutz – Stoppt Angreifer, die Dokumente verschlüsseln, um Lösegeld zu erpressen
- Privacy Protection – Verschlüsselt Tastenanschläge und schützt Webcams vor Spionage

Durch die Übernahme von SurfRight kann Sophos nun auch die oben erwähnte Exploit-Erkennung anbieten. Diese Verfahren können schädliche Aktivitäten zuverlässig mit einer ausreichend niedrigen False-Postive-Rate aufdecken.

Reaktion

Bei der Reaktion auf Bedrohungen werden wir auf eine Reihe von Themen genauer eingehen. Umfasst das Produkt des Anbieters Funktionen wie Malware-Entfernung, Ursachenanalyse, Identifizierung kompromittierter Objekte, Identifizierung verdächtiger Komponenten sowie Scans auf Malware und verdächtige Komponenten auf anderen Geräten und gibt das Produkt umsetzbare Empfehlungen zur Verbesserung der unternehmensweiten Sicherheit, falls schädliche Aktivitäten erkannt wurden?

Malware-Entfernung: Im Sophos Endpoint Agent sind auch Funktionen zur Malware-Entfernung enthalten. Im Falle einer Malware-Erkennung entfernt der Endpoint die Malware also vollständig.

Synchronized Security: Synchronized Security automatisiert die Bedrohungserkennung, -analyse und -reaktion und gestaltet die Bekämpfung von Bedrohungen damit einfacher als je zuvor. Sie können deutlich schneller auf Vorfälle reagieren und Ihre taktischen Ressourcen können sich wieder strategischen Analysen widmen. Synchronized Security ermöglicht es den Endpoint- und Netzwerksicherheitslösungen der nächsten

Generation, wichtige Informationen zu verdächtigen und bestätigten bösartigen Verhaltensweisen im gesamten erweiterten IT-Ökosystemen eines Unternehmens kontinuierlich auszutauschen. Mithilfe einer direkten und sicheren Verbindung namens Sophos Security Heartbeat agiert der Endpoint- und Netzwerkschutz als ein integriertes System, das es Unternehmen ermöglicht, Bedrohungen in Echtzeit ohne zusätzliche Mitarbeiter zu verhindern, erkennen, untersuchen und zu beheben. Wenn die Sophos Next-Gen Firewall beispielsweise eine hochentwickelte Bedrohung oder ein Datenleck erkennt, kann sie automatisch Sophos Security Heartbeat nutzen, um sowohl im Netzwerk als auch am Endpoint mehrere Aktionen auszuführen, die das Risiko mindern und den Datenverlust sofort stoppen. Auf ähnliche Weise kann Synchronized Security automatisch und nahezu sofort einen geschützten Endpoint isolieren, sobald ein Angriff auf diesen erkannt wird. So ist sichergestellt, dass keine vertraulichen Daten abgezogen oder Daten an einen Command-and-Control-Server gesendet werden. Diese Art der Erkennung und sofortigen Reaktion, die ansonsten Wochen oder Monate dauern würden, ist dank Synchronized Security in Sekunden möglich.

Zusammenfassung

Die Meinungen darüber, was unter einem Next-Generation-Endpoint-Security-Produkt zu verstehen ist, gehen heute weit auseinander. Die richtige Technologie zu finden, ist daher besonders schwer. Die immer weiter wachsende Angriffsfläche und höhere Komplexität und Anzahl von Angriffen auf der einen Seite sowie kleine Teams und angespannte Arbeitsmärkte auf der anderen Seite stellen IT-Sicherheitsteams in Unternehmen vor große Herausforderungen.

Unternehmen, die versuchen, dieser Problematik mit verschiedenen Standalone-Produkten Herr zu werden, handeln sich noch mehr Schwierigkeiten ein, statt das Grundproblem zu beseitigen. Wir müssen neue Lösungen implementieren, die einfach und doch effektiv, automatisiert und koordiniert sind, kurz, die über eine innovative Technologie wie Sophos Security Heartbeat synchronisiert sind. Sophos bietet Ihnen jetzt eine solche Lösung und Sie können diese ganz einfach und unverbindlich testen. Informieren Sie sich und testen Sie unsere Next-Gen Endpoint Security – alle Informationen und die Testversion finden Sie unter www.sophos.de/endpoint.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

Oxford, GB | Boston, USA

2016-03-7 SBD-DE (NP)